6.5 Combining Page and Segment Protection

When paging is enabled, the 80386 first evaluates segment protection, then evaluates page protection. If the processor detects a protection violation at either the segment or the page level, the requested operation cannot proceed; a protection exception occurs instead.

For example, it is possible to define a large data segment which has some subunits that are read-only and other subunits that are read-write. In this case, the page directory (or page table) entries for the read-only subunits would have the U/S and R/W bits set to x0, indicating no write rights for all the pages described by that directory entry (or for individual pages). This technique might be used, for example, in a UNIX-like system to define a large data segment, part of which is read only (for shared data or ROMmed constants). This enables UNIX-like systems to define a "flat" data space as one large segment, use "flat" pointers to address within this "flat" space, yet be able to protect shared data, shared files mapped into the virtual space, and supervisor areas.

Table 6-5. Combining Directory and Page Protection

Page Directory Entry		Page Table Entry		Combined Protection	
U/S	R/W	U/S	R/W	U/S	R/W
S-0	R-0	S-0	R-0	S	x
S-0	R-0	S-0	W-1	S	x
S-0	R-0	U-1	R-0	S	x
S-0	R-0	U-1	W-1	S	x
S-0	W-1	S-0	R-0	S	x
S-0	W-1	S-0	W-1	S	x
S-0	W-1	U-1	R-0	S	x

S-0	W-1	U-1	W-1	S	x
U-1	R-0	S-0	R-0	S	x
U-1	R-0	S-0	W-1	S	x
U-1	R-0	U-1	R-0	U	R
U-1	R-0	U-1	W-1	U	R
U-1	W-1	S-0	R-0	S	x
U-1	W-1	S-0	W-1	S	x
U-1	W-1	U-1	R-0	U	R
U-1	W-1	U-1	W-1	U	W

Note

S -- Supervisor
R -- Read only
U -- User
W -- Read and Write
x indicates that when the combined U/S attribute is S, the R/W attribute is not checked.

---

up: Chapter 6 -- Protection
prev: 6.4 Page-Level Protection
next: Chapter 7 -- Multitasking